U.S. Department of the Interior
Office of the Chief Information Officer

Cybersecurity Briefing

November 18, 2015

Agenda

- Cybersecurity
- FITARA Implementation
- Accomplishments
- BIA and BIE services and performance
- Priorities
- Next steps

Background on the OPM/DOI incident

The OPM/DOI cybersecurity breach was identified in April 2015

DOI has been taking the following steps to remediate the incident and improve our cybersecurity posture:

- ✔ Worked with OPM, OMB, DHS and other interagency partners to manage the incident and isolate compromised areas. Met OMB cyber sprint objectives
- ✔ Developed a multi-pronged remediation strategy that includes short and long-term plans to enhance DOI cybersecurity
- ✔ Strengthen our cybersecurity and privacy workforce to effectively address current and future threats

Collaborating to improve cybersecurity

In June 2015, DOI formed the Cyber Advisory Group (Cyber AG), comprised of IT and cybersecurity experts from across the Department to plan and implement cybersecurity improvements.

The Cyber AG and OCIO collaboratively drafted DOI's Cybersecurity Strategic Plan.

Key drivers of DOI's Cybersecurity Strategic Plan

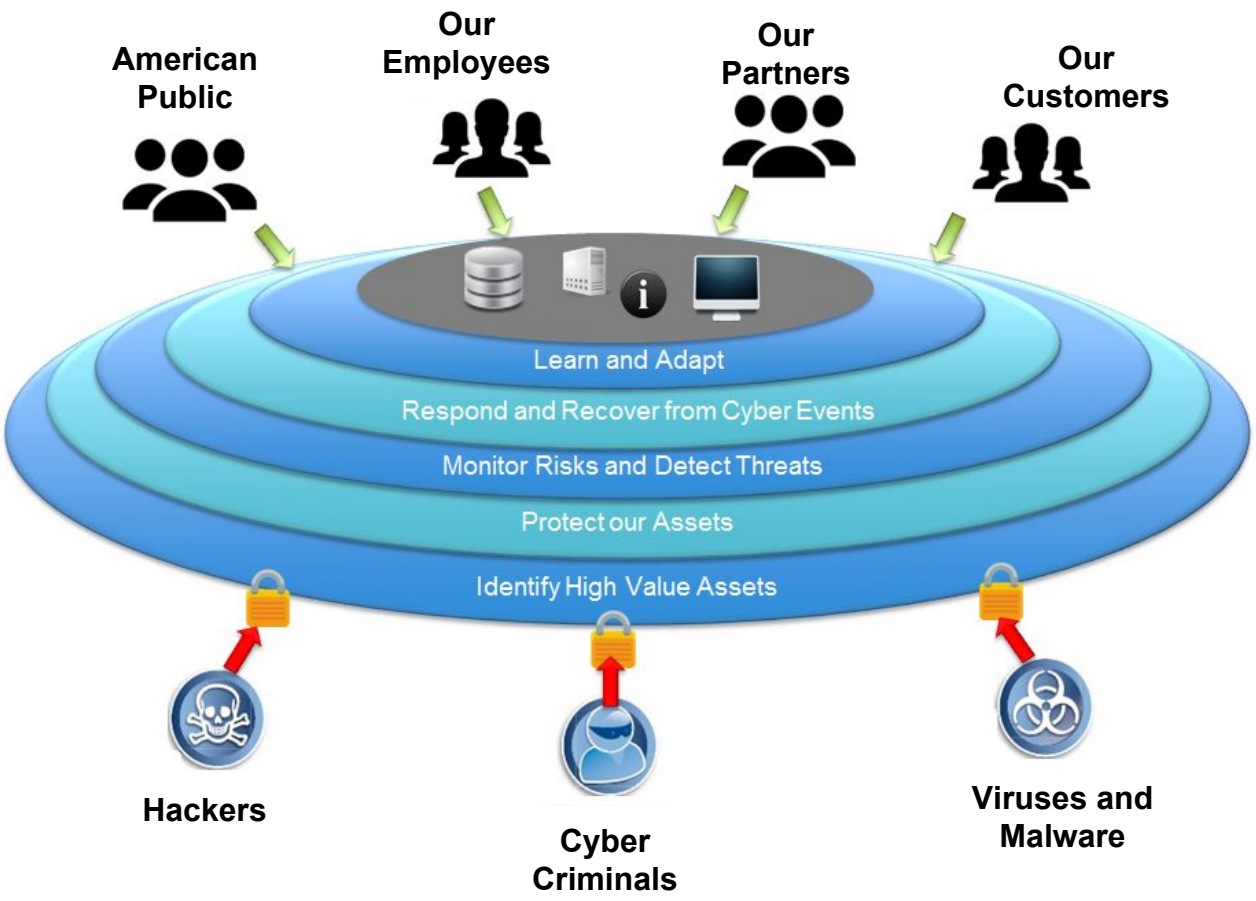
- Secretary's Cybersecurity Directive
- Recent cybersecurity attacks
- Awareness of advanced cyber threats
- DOI OIG's Report on Publicly Accessible IT Systems
- FISMA and FITARA
- EOP policies and guidance

Cybersecurity Plan Vision

Unify the forces of mission and IT to safeguard the Department's high-value information from emerging cyber threats and uphold the trust placed in us by our employees, customers, partners, and American public.

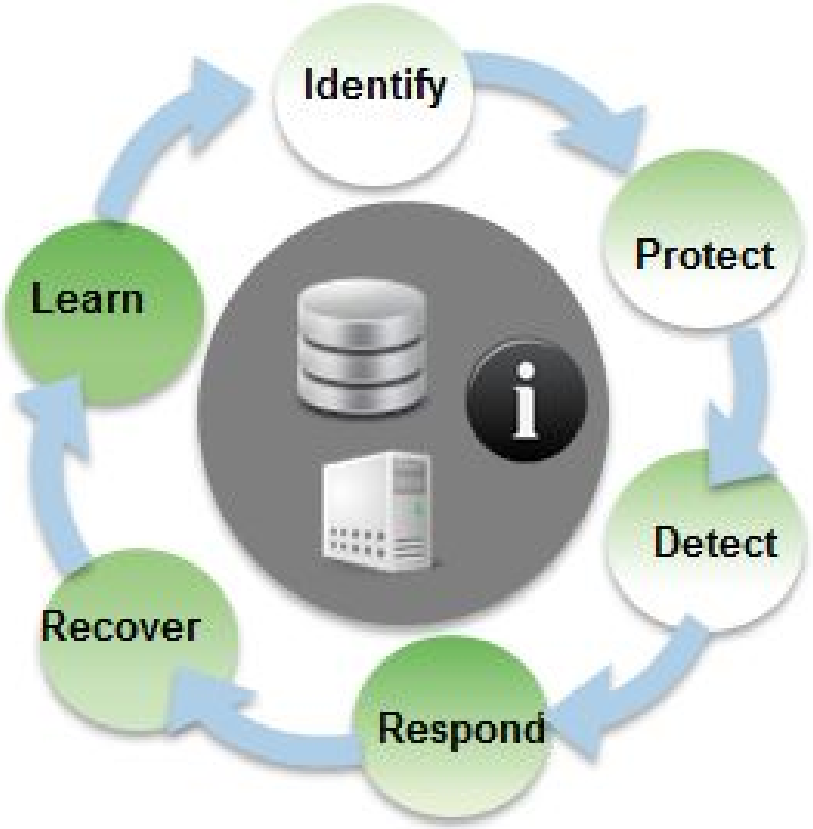
Guiding Principles:

1. Protecting sensitive information
2. Sharing responsibility and collaborating
3. Ensuring transparency and accountability
4. Embracing innovative new technologies



Cybersecurity Plan Framework

The DOI Cybersecurity Framework drives our cybersecurity goals.



- *Identify, Protect, Detect, Respond, and Recover* framework is in accordance with NIST standards.
- *Learn* is a DOI-specific component to highlight our commitment to incorporating lessons learned into all cybersecurity activities.

DOI is continually improving our cybersecurity posture through the cybersecurity framework.

Cybersecurity Plan Goals

1. Identify cybersecurity risks and vulnerabilities
2. Protect the Department's high value assets and information
3. Continuously monitor situational awareness and detect incidents
4. Improve the Department's ability to respond to and recover from cyber events
5. Improve cybersecurity and privacy risk understanding, security posture, and control effectiveness

FITARA Implementation

Federal Information Technology and Acquisition Reform Act

Enacted by Congress on December 19, 2014

- **FITARA outlines specific requirements related to:**
  - Chief Information Officer (CIO) authority enhancements
  - Enhanced transparency and improved risk management in IT investments
  - Portfolio review
  - Expansion of training and use of information technology cadres
  - Federal Data Center Consolidation Initiative
  - Maximizing benefits of the Federal Category Management Initiative
  - Government-wide software purchasing program
- OMB expects DOI to take significant action to implement our plan by December 31, 2015

Key Areas of DOI's FITARA Implementation

1. Issue DOI-wide executive level FITARA guidance
2. Establish a direct line of performance accountability
   a. CIO and future bureau/office Associate CIOs (ACIO)
   b. Chief Information Security Officers (CISOs)
   c. Privacy Officers
3. Centralize authority of information management and technology (IMT) under the future bureau/office ACIO, respectively
4. Update planning and budgeting policies, processes, and procedures for IMT investments and spending
5. Update policies, processes, and procedures for IMT acquisitions

Accomplishments

Overall Cybersecurity Accomplishments

Formed the Cyber Advisory Group (Cyber AG)

Drafted Cyber Security Strategic Plan and Budget Requests

Submitted FITARA Plan to OMB

Cyber Sprint Accomplishments

Reduced Privileged Users by 21% - from 7,477 on 7/15 to 5,848 on 8/28

PIV-enforced Privileged Users & Unprivileged Users meet OMB requirements

Reduced the number of unscanned hosts by 99%

Deployed tools that give us visibility into the network to detect suspicious activity

Completed High Value Asset (HVA) inventory and prioritized HVAs by bureau

Resolved patching issues with Windows 2003 & ColdFusion

BIA and BIE Services and Performance

- Provides IT and business resources used daily by over 13,000 individuals to perform mission support activities for Indian Country
- Owns and operates a DOI Core Data Center in Albuquerque, NM
- Identifies, tracks, and remediates critical vulnerabilities by continuously monitoring the BIA Network
- Completed a 100% physical assessment of 177 Bureau of Indian Education (BIE) schools to proactively identify and prioritize infrastructure and technology upgrade needs
- Initiated the BIE Education Native American Network (ENAN II) Cyber Security Project

Strategic Priorities

1. FITARA Implementation
2. Cybersecurity
   a. Hosting (Data Center Consolidation and Cloud)
   b. Telecommunications
   c. Secure Mobility
3. Strategic Sourcing and Category Management
4. Wildland Fire IT
5. Revenue Management Shared Services

Identified as BY 2018 and BY 2019 IT Strategic Priorities

Other areas of focus (pending approval)

- Information Rights Management
- Department-wide Application Whitelisting
- Network-Based Forensics
- Web Application Scanning

Next steps for BIA and BIE

- Complete assessment reports from 177 BIE school site visits and utilize data to:
  - Develop IT support standards
  - Assist future support prioritization decisions
  - Conduct a gap analysis between current BIE school IT solutions and what's required to meet Common Core standards
- Continue to improve overall Indian Affairs IT security posture
  - Continue cyber sprint activities, including decreasing privileged users
  - Implement DOI's Cybersecurity Strategic Goals
  - Bolster strong collaboration between mission staff and IT staff
- Continue to partner with OCIO to implement forthcoming FITARA guidance and cybersecurity priorities

Questions?

U.S. Department of the Interior
Office of the Chief Information Officer